REPRINTED WITH PERMISSION FROM NCEES Licensure Exchange, August 2017

AN OFFICIAL NCEES PUBLICATION FOR THE EXCHANGE OF INFORMATION, OPINIONS, AND IDEAS REGARDING THE LICENSURE OF ENGINEERS AND SURVEYORS

Licensure EXCHANGE

AUGUST 2017
Volume 21, Issue 4

NCEES

JASON KENT, P.E.
OREGON BOARD OF EXAMINERS FOR ENGINEERING AND LAND SURVEYING MEMBER

RON SINGH, P.L.S.
OREGON BOARD OF EXAMINERS FOR ENGINEERING AND LAND SURVEYING PAST MEMBER

UNDERSTANDING DIGITAL SIGNATURES

NCEES *MODEL LAW* 140.10(C) REQUIRES DOCUMENTS to be sealed, signed, and dated. Traditional handwritten signatures on physical engineering documents worked well when documents were written or drawn by hand. They also worked reasonably well in the early days of using computers to simply speed up the document-development process, with the intent of producing final documents on paper. However, computer use has progressed into an era in which electronic documents are transmitted, reviewed and approved, used during the bidding process and for stakeless construction, and archived for future retrieval.

Applying a handwritten signature to these electronic files requires printing the document, signing it, and then scanning it back into an electronic file. This process loses the electronic file's native format and any imbedded intelligence. It is also time consuming and unnecessary.

Electronic vs. digital signatures

The terms *electronic signature* and *digital signature* are often used interchangeably. In the information security world, however, the two terms are distinctly different. An electronic signature may include scanned images of handwritten signatures or typed notations such as "/s/ Jane Doe" without any authentication or encryption system included. For example, a drawing set that uses computer-aided drafting with a digital reproduction of an engineer's or surveyor's seal and signature across the seal is an electronic signature. This type of signature is neither a handwritten signature nor a digital signature, and it is digitally insecure. Similarly, a signature block on an email message may also be considered an electronic signature.

The term *digital signature* is more properly used to describe a signature system applied to an electronic document that uses specific technical processes to provide significant added signer authentication, document authentication, document encryption (if necessary), and efficiency. Instead of using pen and paper, a digital signature uses digital keys to attach the identity of the signer to the document and record a binding commitment to the content of the document. Digital signatures enable authentication of digital documents, assuring the recipient of the sender's identity and the document's integrity. A digital signature provides who signed the digital file. A time stamp of that digital signature provides when the digital file was signed.

Why use digital signatures?

A digital signature provides a greater degree of security than a handwritten signature does. The recipient of a digitally signed document can verify that the document originated from the person whose signature is attached and that the document has not been altered (intentionally or accidentally) since it was signed.

Digital signature technology is not an emerging technology. It has undergone thorough research and development

continued on page 2

over the past two decades. Several national and international standards allow digital signatures. These standards were developed and are accepted by many corporations, banks, and government agencies. A robust digital signature system is capable of creating a signature unique to the person using it, capable of verification, under the sole control of the person using it, and linked to the document so that the digital signature is rendered invalid if any part of the document is altered. These requirements are listed in NCEES *Model Rules* 240.20 C8. Less-robust digital signature systems that do not provide these benefits should be avoided.

What is needed to create a digital signature?

Creating a digital signature requires software, a signing certificate, and optionally, hardware to provide further security with a signer's private key. Creating the signing certificate involves making a public–private digital key pair and, optionally, obtaining the services of a certificate authority.

The public key certificate creates proof of the signer's identity and is made available to anyone who needs to verify the signature. Also called a signer's certificate, the public key certificate is created by the combination of the public key and proof of identity.

The document is signed with the private key, which is kept by only the signer. The public and private keys are related mathematically. Knowing the public key allows a signature to be verified but does not allow new signatures to be created. If the private key is not kept private, someone could create the original signer's signature on a document without consent. It is critical to keep the private key secret.

To verify a digital signature, the verifier must have access to the signer's public key and have assurance that it corresponds to the signer's private key. This assurance can be provided by using a trusted third party to associate an identified signer with a specific public key. That trusted third party is known as a certification authority.

To associate a key pair with a prospective signer, the certification authority issues a certificate—an electronic record that lists a public key as the subject of the certificate—and confirms that the prospective signer identified in the certificate holds the corresponding private key. The certification authority performs a background check on each person who is assigned a signing certificate.

A self-signed certificate is one that is created by the individual signer without the services of a certification authority. It should be avoided. Digital IDs provided by third parties are generally considered more secure because an independent certification authority has ratified them. A signature applied using a self-signed certificate signature tells document recipients, "This document is valid, and I am authorized to sign it," while a signature applied using a third-party digital ID tells them, "This document is valid, I am authorized to sign it, and [certification authority] verifies my identity." This additional assurance can make a big difference when it comes to legal documents or documents sent out to a wide audience.

Security of digital signatures

Digital signatures provide a secure, efficient, and convenient process for sealing a document pursuant to NCEES *Model Law* 140.10 C. For recipients of digitally signed documents, they also provide assurance that a document is authentic and original. Digital signature technology is well established and accepted in a multitude of settings. In addition, certification authorities have developed technologies that can evolve to meet the scenarios set forth in *Model Rules* 240.20 C.

Member boards should recognize that digital signature technology is not universally understood, and the terms *digital signature* and *electronic signature* are commonly confused. Boards and licensees should be aware of the distinctions between these strategies and recognize the insecurities of using electronic signatures as well as the robustness and security afforded by digital signature technology.